Faculty of Computing

Computer Networks

Enterprise Network Design – Supermarket

CN 301.3 – Advanced Routing and Switching

Table of Contents

Introduction

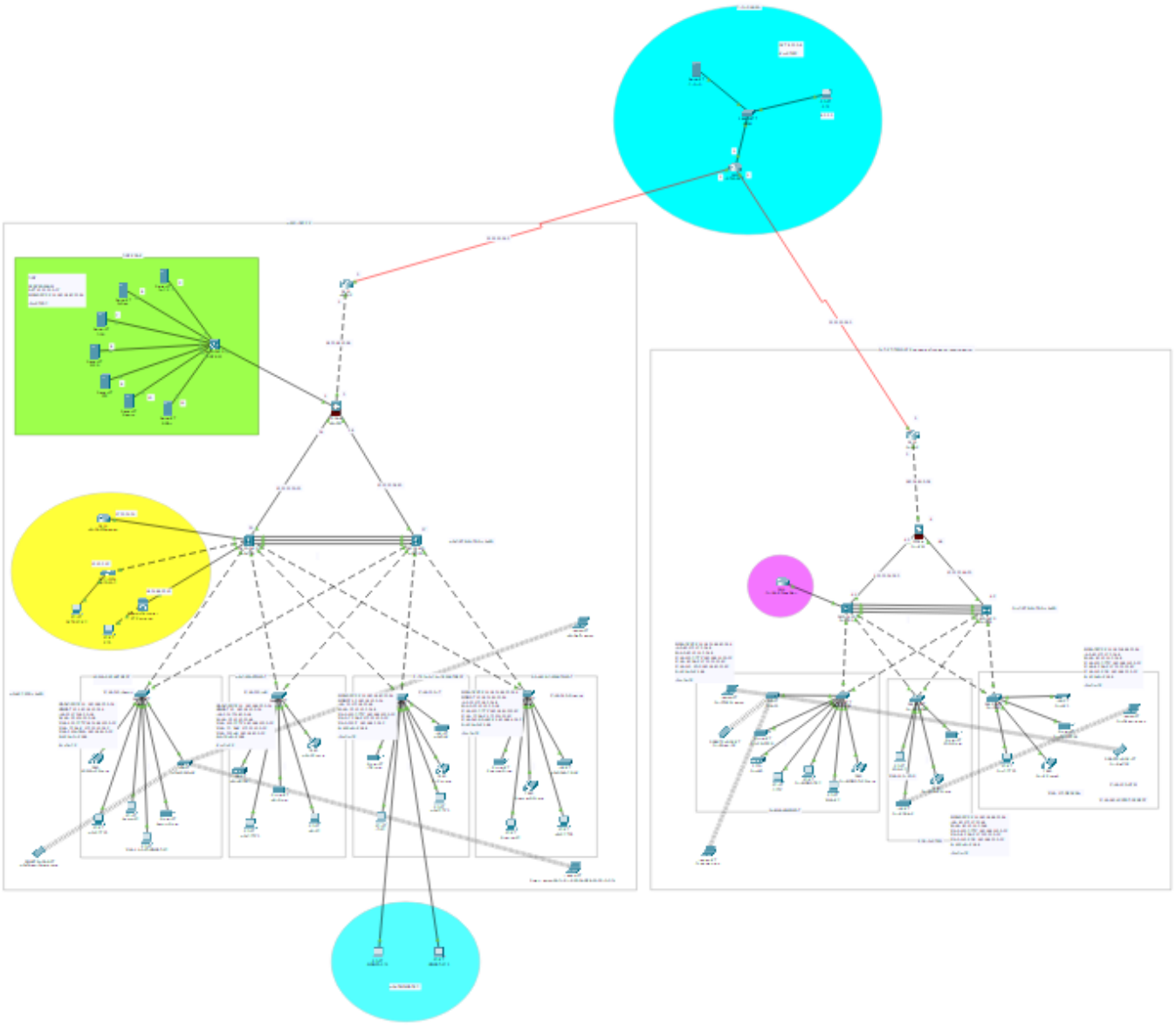
In today's retail industry, which is led by digital technologies, a robust and scalable ICT infrastructure is essential for the delivery of seamless operations, efficient communication, and high-quality customer service. The project is based on the redesign of the ICT infrastructure of a supermarket chain with stores of varying sizes small, standard, and mega distributed across multiple regions.

The key necessity of the new design is to enable operational efficiency, centralized control, scalability, and future-proofing. The proposed solution interconnects all the branches securely to the Head Office (HO) at Peliyagoda through IPsec VPN tunnels. This enables secure communication across the network while permitting remote troubleshooting, centralized access to services, and policy enforcement from the HO.

All the mission-critical services such as DHCP, DNS, VoIP, and cloud-based application support are maintained at the head office. The infrastructure is designed for easy upgrades or downgrades at the outlet level without requiring major structural changes supporting dynamic business needs.

The network solution also offers appropriate segmentation for security, firewall protection, PoE-based CCTV connectivity, and wireless access based on the size of the outlet. The design was implemented and tested using Cisco Packet Tracer, following the principles of routing, switching, and secure communications to meet current as well as future requirements of the supermarket chain.

Network Diagram



Network Segmentation & VLAN Structure

Head Office VLANs

VLAN ID	Pool Name	Subnet	Department/Function
10	HQ-MGMNT-POOL	192.168.10.0/24	HQ IT Management
20	HQ-LAN-POOL	172.17.0.0/16	Wired Users (General)
50	HQ-WLAN-POOL	10.10.0.0/16	Wireless Devices
70	HQ-VoIP-POOL	172.20.10.0/25	IP Phones
100	HQ-CCTV-POOL	192.168.100.0/25	CCTV Systems
210	ADMIN-POOL	192.168.1.0/25	Admin Department
220	HR-POOL	192.168.2.0/25	HR Department
230	IT-POOL	192.168.3.0/25	IT Department
240	FINANCE-POOL	192.168.4.0/25	Finance Department
11	HQ-MNG-DEVICE-POOL	192.168.5.0/24	Management devices

Outlet VLANs

VLAN ID	Pool Name	Subnet	Department/Function
60	OU-LAN-POOL	172.17.0.0/16	Wired Users (General)
90	OU-WLAN-POOL	10.11.0.0/16	Wireless Devices
80	OU-VoIP-POOL	172.30.20.0/25	IP Phones
110	OU-POS-POOL	192.168.20.0/25	POS System
100	OU-CCTV-POOL	192.168.110.0/25	CCTV Systems
11	OU-MNG-DEVICE-POOL	192.168.60.0/24	Management devices

DMZ & External

Name	Subnet	Use
DMZ	10.20.20.0/27	Central Servers (HQ)
CLOUD-AREA	8.0.0.0/8	External Cloud Network (for ref)

IP Addressing Plan

Servers (in HQ DMZ)

Server Type	IP Address
DHCP	10.20.20.5
SYSlog	10.20.20.6
DNS	10.20.20.7
Web	10.20.20.8
NTP	10.20.20.9
RADIUS	10.20.20.10
EMAIL	10.20.20.11

ISP Routers & Firewalls

Device	Public IP	Subnet
HQ Firewall	192.248.1.2	255.255.255.240
Outlet FW	192.248.1.4	255.255.255.240
HQ ISP Router	192.248.1.1	255.255.255.240
Outlet Router	192.248.1.3	255.255.255.240

Controllers

Device	IP
CISCO-WLC	10.10.0.15/16
Network Controller	192.168.50.10/24

Head Office Network Architecture

The Head Office employs a modular, layered enterprise network model that integrates redundancy, inter-VLAN routing, and segregated security zones. The infrastructure supports scalable expansion and high availability for critical business services.

Core Components:

1. **Edge Layer:**

   - The edge layer at the Head Office serves as the primary gateway between the internal enterprise network and the public internet. It consists of an ISP Router and an enterprise-grade firewall (Cisco ASA 5506-X)
   - HQ ISP Router connects to the public internet with a 192.248.1.0/28 subnet, providing routing to the HQ public-facing firewall (5506-X).
   - The firewall enforces stateful packet inspection, NAT (Network Address Translation), and Access Control List (ACL) enforcement. This firewall also terminates IPsec VPN tunnels from all branch outlets, securing branch-to-HQ communication over the public internet
   - Using a firewall like the ASA 5506-X at the edge ensures deep packet inspection and IPsec VPN support, and modular policy control, which is critical in a multi-branch enterprise network for maintaining data confidentiality and network integrity. The 192.248.1.0/28 subnet allocation balances efficient public IP use while allowing growth.

2. **DMZ Segment (De-Militarized Zone):**

   - Located behind the firewall in a semi-trusted security zone using subnet 10.20.20.0/27.
   - Hosts critical servers:
     - ✓ DHCP, DNS, Email, Web, Syslog, RADIUS, NTP
     - ✓ Servers are individually firewalled via internal firewall rules to minimize lateral threats.
   - Traffic to/from the DMZ is strictly controlled using zoned firewall policies and access control lists (ACLs).
   - Placing public-facing and core servers (DNS, Web, Email, SYSLOG, NTP, DHCP, RADIUS) in the DMZ reduces attack surfaces within the LAN. The 10.20.20.0/27

subnet is isolated, and granular ACLs help enforce east-west traffic controls, reducing risk from lateral movement.

3. **Distribution Layer:**

- ❖ The distribution layer consists of dual Layer 3 core switches (L3-SW1 and L3-SW2), which act as the routing backbone for the entire head office LAN
- ❖ These switches are configured with HSRP for gateway redundancy or EtherChannel for high-availability uplinks. They handle inter-VLAN routing , maintain OSPF adjacency with the firewall, and aggregate connections from all departmental switches
- ❖ By hosting routing intelligence and implementing ACLs and QoS policies, this layer ensures secure, efficient, and resilient traffic flow. The use of OSPF provides dynamic adaptability, while redundancy ensures no single point of failure, vital for uninterrupted business operations.

4. **Access Layer (Department-Level Switching):**

- ❖ The access layer includes dedicated Layer 2 managed switches per department, providing endpoint connectivity for PCs, IP phones, printers, and access points
- ❖ Each department connects through its own dedicated Layer 2 managed switch, segmented by VLAN (VL-210-240) enabling segmented traffic, broadcast domain isolation, and policy enforcement
- ❖ VoIP, CCTV, Wireless are also segmented to prioritize bandwidth and security. All devices obtain IPs via DHCP relay from a centralized server in the DMZ, and CAPWAP-enabled Access Points are centrally managed by a Wireless LAN Controller (WLC). This layered segmentation enhances performance, security, and simplifies troubleshooting.
- ❖ Virtual LANs in access layer
  - ✓ VLANs 210–240 for Admin, HR, IT, Finance
  - ✓ VLAN 10 for IT Management.
  - ✓ VLAN 11 for MNG-DEVICES
  - ✓ VLAN 50 supports wireless devices via centralized WLC (10.10.0.15).
  - ✓ VLAN 70 carries VoIP traffic, separated using Voice VLAN tagging for QoS (802.1p/DSCP).
  - ✓ VLAN 100 is reserved for CCTV surveillance systems, isolated from user traffic.

- ❖ Devices per department include:
  - ✓ PCs (Dynamic IP via DHCP relay)
  - ✓ IP Phones (registered to central VoIP server)
  - ✓ Network printers
  - ✓ Access Points (CAPWAP-controlled by WLC)
  - ✓ CCTV IP cameras (streamed and archived to storage server)

5. **Voice Infrastructure:**

- ❖ VoIP Gateway connects analog/digital telephony to IP-based SIP infrastructure.

Branch Outlet Network Architecture

The Outlet's network is a compact edge-network topology, designed to function autonomously while remaining fully integrated with the HQ via a secure site-to-site IPsec VPN tunnel.

The branch outlet's edge layer is designed for autonomous operation while maintaining secure connectivity to the HQ. It comprises an ISP Router and an enterprise firewall, which together establish and maintain an IPsec VPN tunnel to the HQ firewall

1. **Edge Components:**
    - ❖ Outlet ISP Router → connects to the Outlet Firewall, which performs:
        - ✓ Inbound/outbound firewalling for segmented VLAN traffic
        - ✓ NAT for internet access for local devices
        - ✓ DHCP relay back to HQ server via VPN tunnel
    - ❖ This tunnel allows secure routing of VLAN-tagged traffic, DHCP relay, and access to centralized services (authentication, WLC, DNS). The firewall also handles NAT, port-based ACLs, and filters both inbound and outbound traffic to protect local resources
    - ❖ Deploying firewall functions at the branch ensures local threat containment, WAN independence, and maintains data confidentiality across the WAN.

2. **Distribution Layer:**
    - ❖ The Distribution Layer at the branch outlet is implemented using two redundant multilayer switches (MLS) configured with EtherChannel and Hot Standby Router Protocol (HSRP) to ensure both high availability and fault tolerance
    - ❖ These switches serve as the backbone of the outlet's internal network, handling inter-VLAN routing, load balancing, and gateway redundancy for end devices. By employing OSPF (Open Shortest Path First) as the dynamic routing protocol, the outlet ensures efficient route propagation and convergence, especially between local VLANs and the HQ via the site-to-site VPN tunnel.
    - ❖ The MLS pair also enforces Access Control Lists (ACLs) to control traffic flow between VLANs, applying granular security policies such as restricting POS systems from directly communicating with management or CCTV segments
        - ❖ Trunk links from the distribution switches carry all outlet VLANs (e.g., VLAN 60 LAN, VLAN 110 for POS, VLAN 80 for VoIP, etc.) down to the access layer switches

3. **Access Layer & VLAN Structure:**

Function	VLAN	Devices Connected
OU-LAN	60	WAN PC, Mgmt PC, Printer, IP Phone, AP, CCTV
MNG-DEVICE	11	Every Network Devices
POS System	110	POS PC, Receipt Printer
OU-WLAN	90	All APs operate in lightweight mode under HQ WLC over CAPWAP
IP Telephony	80	VoIP traffic isolated using voice VLAN settings and QoS policies
CCTV	100	IP Cameras stream to HQ or local NVR for recording

- ✓ Access Points broadcast segmented SSIDs with WPA2-Enterprise encryption, authenticated via RADIUS server at HQ.
- ✓ Local switch ports are configured with port-security,
- ✓ All user devices receive IP addresses via DHCP relay, with DHCP requests securely tunneled to the HQ server
- ✓ This access layer supports endpoint segmentation.

4. **Voice Infrastructure:**

- ❖ The branch outlet uses Voice VLAN 80 to isolate voice traffic and ensure QoS for IP phones. Phones register to the VoIP Gateway.

Interconnectivity & VPN Architecture

To connect the **Head Office (HQ)** and **Outlet (OU)** securely, we set up a **Site-to-Site IPsec VPN tunnel** using their public IPs. This allows both locations to share resources like servers, storage, and services (e.g., DHCP, DNS, WEB SERVER, SYSLOG, NTP). Instead of static routes, we use **OSPF** (a dynamic routing protocol) to handle all internal network routes automatically.

VPN Tunnel Setup

Location	Device	Public IP
HQ	Router	192.248.1.1
OU	Router	192.248.1.3

- **VPN Type**: Site-to-Site IPsec VPN
- **Encryption**: Strong encryption (aes 256)

To allow full communication between all the networks at the Head Office (HQ) and Outlet (OU), an **Access Control List (ACL 130)** was configured on both VPN routers.

This ACL defines the **"interesting traffic"** which will be encrypted and sent over the VPN tunnel.

ACL 130 permits traffic between every required internal subnet, including:

- HQ VLANs: 10.10.0.0/16, 172.16.0.0/16, 192.168.1.0/25, 192.168.2.0/25, etc.
- OU VLANs: 10.11.0.0/16, 172.17.0.0/16, 192.168.20.0/25, 192.168.110.0/25, etc.
- DMZ subnet: 10.20.20.0/27 (for DHCP, DNS, Web, NTP, etc.)

These ACLs were mirrored on both the HQ and OU routers to ensure **bidirectional access**, allowing both sides to access shared services like DNS, DHCP, Syslog, VoIP, and Email.

This ACL structure ensures that **only permitted subnets can communicate**, helping enforce security while enabling full service access over the VPN.

Routing with OSPF

- We use **OSPF** to share all the internal subnets between HQ and OU.
- Both HQ and OU routers/firewalls run OSPF **in Area 0**.
- No need to manually add routes — OSPF automatically shares and updates routes.

Subnets Shared by OSPF:

- **From HQ**:
  - WLAN: 10.10.0.0/16
  - LAN: 172.16.0.0/16
  - VoIP: 172.20.10.0/25
  - CCTV, Management, MNG-Device, Departments: 192.168.x.x ranges

- **From OU**:
  - WLAN: 10.11.0.0/16
  - LAN: 172.17.0.0/16
  - VoIP: 172.30.20.0/25
  - POS, CCTV: 192.168.x.x ranges

Services Used Over VPN

Service	Location	Used by
DHCP Server	HQ (DMZ)	Both HQ & OU
DNS Server	HQ (DMZ)	Both HQ & OU
NTP Server	HQ (DMZ)	Both HQ & OU
RADIUS Server	HQ (DMZ)	Both HQ & OU
Email/Web	HQ (DMZ)	Both
WLC	HQ (10.10.0.15)	Both Wireless Access Points
Netwotk Controller	HQ (192.168.50.10)	Both Wireless Access Points

Security & Monitoring

- Access Control Lists (ACLs) are configured at the distribution layer to restrict inter-VLAN traffic and control access to essential services such as DHCP and DNS
- Wireless security is enforced using WPA2-Enterprise encryption with centralized **RADIUS authentication** via the HQ server, ensuring only authenticated users connect to the APs.
- Unused switch ports are assigned to a non-routable blackhole VLAN (VLAN 199) and administratively shut down to eliminate physical attack vectors.
    - ✓ These measures collectively enhance the outlet's security posture by combining network segmentation, role-based access, and endpoint isolation.
- To ensure proactive network oversight, the Head office and outlet's monitoring system is integrated with a **centralized Syslog server** hosted in the DMZ of the Head Office
    - ✓ All routers, Layer 3 switches, and Layer 2 switches at the outlet are configured to forward system logs and critical event data to this server. This setup enables administrators to track configuration changes, interface status, VPN tunnel health, and potential security alerts in real time.
- **Network Time Protocol (NTP**) is deployed on all network devices to make time synchronization a necessity in accurate log correlation, secure communication protocols, and forensic analysis.
    - ✓ A Network Controller is installed for centralized monitoring, visualization, and simple management of network performance, client behavior, and policy enforcement.

Servers & Centralized Services

All core services are located in the HQ DMZ Zone:

Server	Function
DHCP Server	Dynamically allocates IP addresses to outlet and HQ devices based on predefined VLAN pools, reducing manual configuration
DNS Server	Handles internal name resolution, allowing seamless communication between hosts.
Web Server	Hosts internal applications and staff portals, while the Email server manages secure internal email communications
Email Server	Manage and facilitate internal and external email communication within the organization
RADIUS Server	Provides centralized user authentication for wireless devices
Syslog Server	Aggregates logs from network devices for centralized monitoring and audit trails
NTP Server	NTP Server is to synchronize the clocks of devices on a network to a common, accurate time source

Packet Tracer Implementation

We implemented the network in Cisco Packet Tracer, including:

Edge Security & Connectivity:

- **Cisco ASA 5506-X Firewall:** Deployed at both the HQ and Outlet edge to act as the IPsec VPN endpoint, enforce security policies via ACLs and stateful inspection, and perform NAT.
- **Cisco 2911 Router:** Utilized to simulate the ISP-facing routers at both HQ and the Outlet, handling basic WAN connectivity and routing towards the respective firewalls.

HQ Core & Switching:

- **Cisco Catalyst 3650-24PS Multi-Layer Switch**: Two units implemented as the redundant HQ Core layer, performing high-speed Layer 3 Inter-VLAN routing (using SVIs), providing gateway redundancy via HSRP, and configured with EtherChannel for inter-switch link aggregation. Their PoE capability supports directly connected APs or phones if needed at the core level.
- **Cisco Catalyst 2960 Switch:** Employed as Layer 2 Access Switches at both HQ and the Outlet(s) to provide end-device connectivity, assign ports to specific VLANs, implement port-security, and deliver PoE (assuming PoE capable models) to devices like IP Phones and Access Points.

Wireless Networking:

- **Cisco 2504 Wireless LAN Controller (WLC):** Centralized within the HQ server farm to manage all lightweight access points across the network, configure SSIDs, and enforce wireless security policies.
- **Lightweight Access Points (LAP-PT):** Deployed at HQ and the Outlet(s) to provide wireless coverage for Staff and Customer SSIDs, forwarding traffic back to the WLC

Centralized Services & Management:

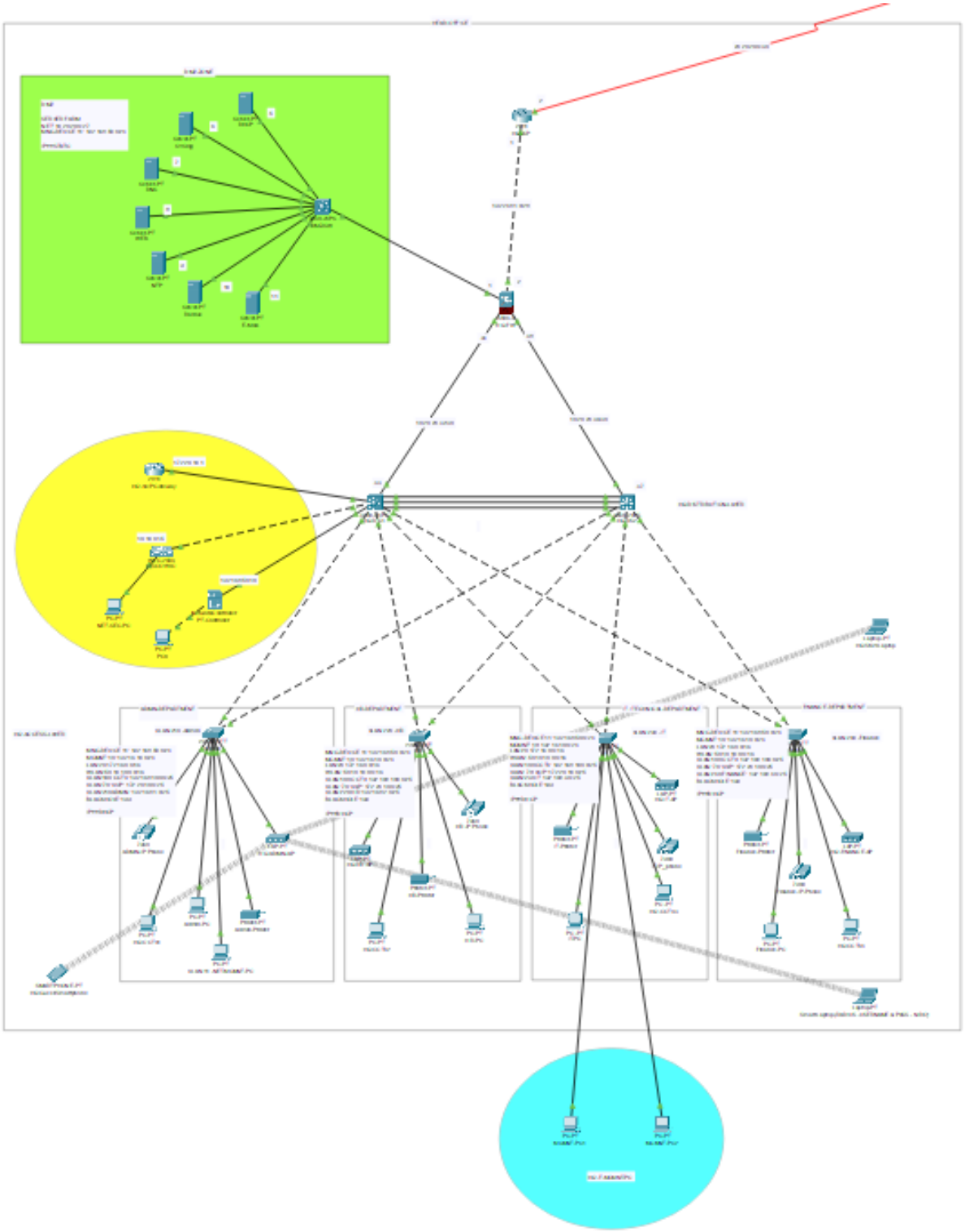
- **Servers (Server-PT):** Multiple instances used within the HQ DMZ/Server Farm to simulate critical services like DHCP, DNS, AAA (RADIUS), Web Server (POS Backend/Portal), NMS (Network Controller simulation), NTP(Network Time)
- **Network-Controller:** Responsible for managing and monitoring all network devices.

End Devices for Realism & Testing:

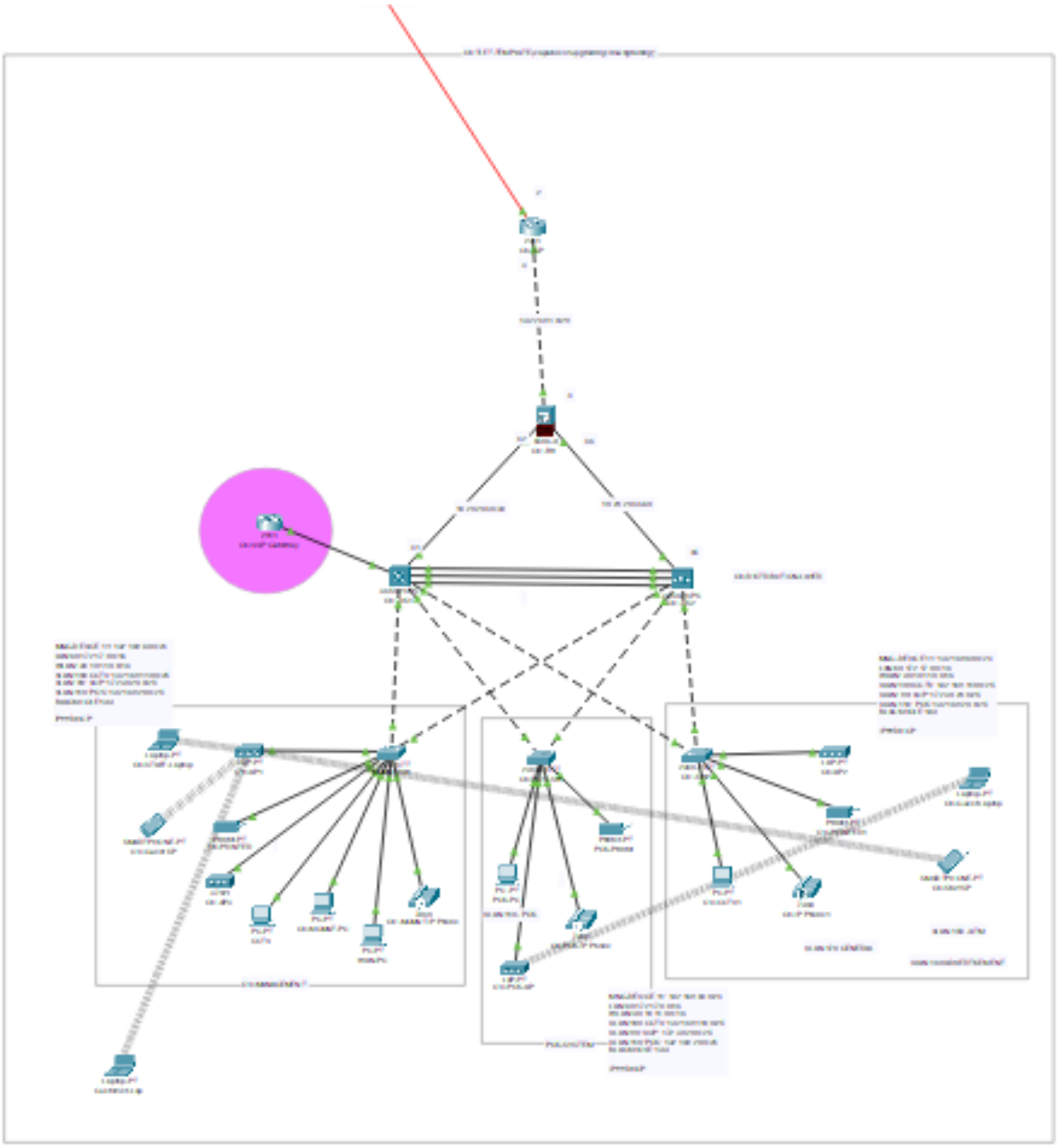
- PCs (PC-PT): Representing wired staff workstations, POS Terminals, and management stations.
- Laptops (Laptop-PT): Simulating staff mobile devices and customer WiFi clients.
- IP Phones (7960 model): Deployed for VoIP testing, registering to the simulated call manager and utilizing the Voice VLAN.
- Smartphones (Smartphone-PT): Used to test wireless connectivity, particularly for guest or staff mobile scenarios.
- Printers (Generic Printer/PC-PT): Simulated devices connected within the secure ports

Screenshots

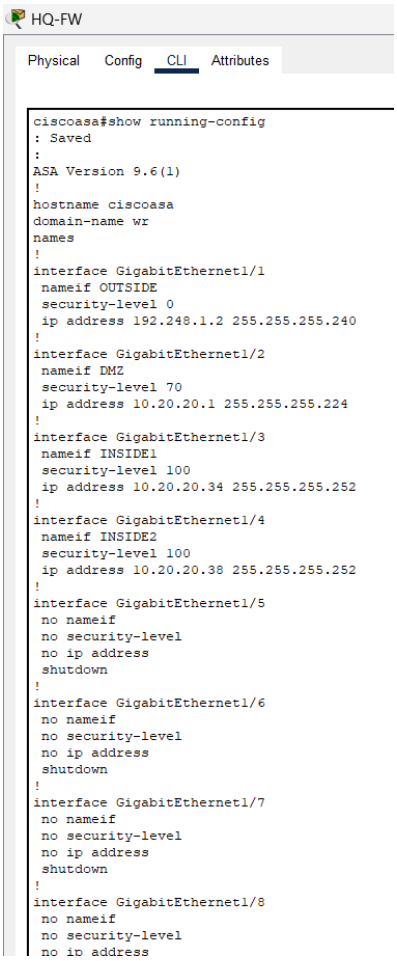
HO layout

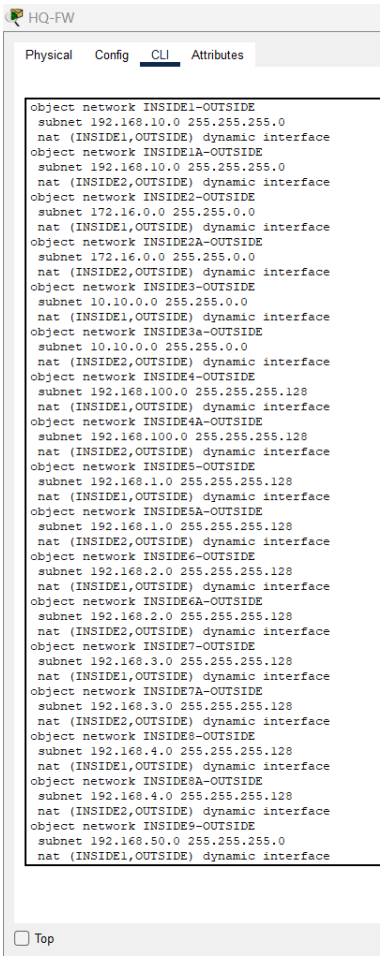


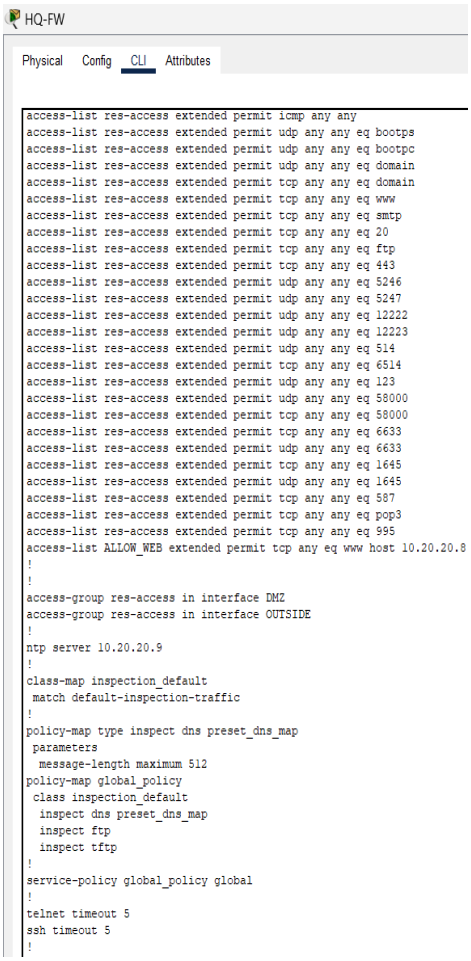
Sample outlet (Small, Standard, Mega template)



HQ Firewall Configurations








```
!
service-policy global_policy global
!
telnet timeout 5
ssh timeout 5
!
!
!
!
router ospf 15
 router-id 3.2.4.1
 log-adjacency-changes
 network 192.248.1.0 255.255.255.240 area 0
 network 10.20.20.0 255.255.255.224 area 0
 network 10.20.20.32 255.255.255.252 area 0
 network 10.20.20.36 255.255.255.252 area 0
!
ciscoasa#
```

- ✓ The same configurations configured on Outlet firewall

HQ MLS Configurations (Distribution layer)

HQ-DS1

Physical Config CLI Attributes

```
ip ssh version 2
no ip domain-lookup
ip domain-name shan.com
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface Port-channel1
 switchport mode trunk
!
interface GigabitEthernet1/0/1
 no switchport
 ip address 10.20.20.33 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet1/0/2
 switchport mode trunk
!
interface GigabitEthernet1/0/3
 switchport mode trunk
!
interface GigabitEthernet1/0/4
 switchport mode trunk
!
interface GigabitEthernet1/0/5
 switchport mode trunk
!
interface GigabitEthernet1/0/6
 switchport access vlan 70
 switchport mode access
 switchport voice vlan 70
!
interface GigabitEthernet1/0/7
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
 switchport access vlan 50
 switchport trunk native vlan 50
 switchport mode trunk
 spanning-tree portfast
 spanning-tree bpduguard enable
!
```

HQ-DS1

Physical Config CLI Attributes

```
interface GigabitEthernet1/0/21
 switchport mode trunk
 channel-group 1 mode active
!
interface GigabitEthernet1/0/22
 switchport mode trunk
 channel-group 1 mode active
!
interface GigabitEthernet1/0/23
 switchport mode trunk
 channel-group 1 mode active
!
interface GigabitEthernet1/0/24
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 mac-address 00e0.f77a.6901
 ip address 192.168.10.3 255.255.255.0
 ip helper-address 10.20.20.5
 standby 10 ip 192.168.10.1
!
interface Vlan11
 mac-address 00e0.f77a.6902
 ip address 192.168.50.6 255.255.255.0
 ip helper-address 10.20.20.5
 standby 11 ip 192.168.50.1
!
interface Vlan20
 mac-address 00e0.f77a.6903
 ip address 172.16.0.3 255.255.0.0
 ip helper-address 10.20.20.5
 standby 20 ip 172.16.0.1
!
interface Vlan50
 mac-address 00e0.f77a.6904
 ip address 10.10.0.3 255.255.0.0
 ip helper-address 10.20.20.5
 standby 50 ip 10.10.0.1
!
```

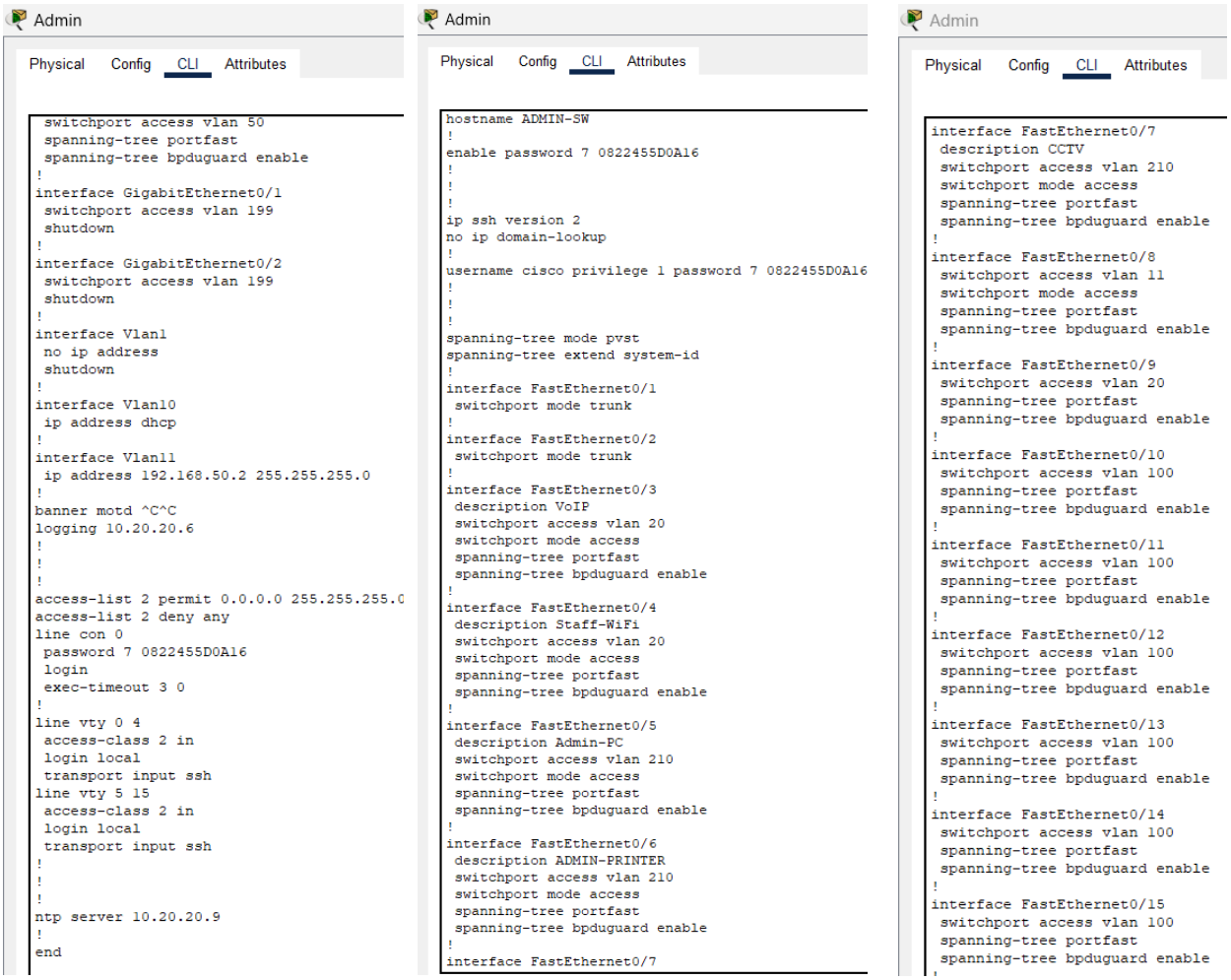
HQ-DS1

Physical Config CLI Attributes

```
interface Vlan70
 mac-address 00e0.f77a.6905
 ip address 172.20.10.3 255.255.255.128
 ip helper-address 172.16.10.1
 ip helper-address 172.20.10.1
!
interface Vlan100
 mac-address 00e0.f77a.6906
 ip address 192.168.100.3 255.255.255.128
 ip helper-address 10.20.20.5
 standby 100 ip 192.168.100.1
!
interface Vlan210
 mac-address 00e0.f77a.6907
 ip address 192.168.1.3 255.255.255.128
 ip helper-address 10.20.20.5
 standby 210 ip 192.168.1.1
!
interface Vlan220
 mac-address 00e0.f77a.6908
 ip address 192.168.2.3 255.255.255.128
 ip helper-address 10.20.20.5
 standby 220 ip 192.168.2.1
!
interface Vlan230
 mac-address 00e0.f77a.6909
 ip address 192.168.3.3 255.255.255.128
 ip helper-address 10.20.20.5
 standby 230 ip 192.168.3.1
!
interface Vlan240
 mac-address 00e0.f77a.690a
 ip address 192.168.4.3 255.255.255.128
 ip helper-address 10.20.20.5
 standby 240 ip 192.168.4.1
!
router ospf 15
 router-id 2.1.2.1
 log-adjacency-changes
 network 10.20.20.32 0.0.0.3 area 0
 network 192.168.10.0 0.0.0.255 area 0
 network 172.16.0.0 0.0.255.255 area 0
 network 10.10.0.0 0.0.255.255 area 0
 network 192.168.100.0 0.0.0.127 area 0
 network 192.168.1.0 0.0.0.127 area 0
 network 192.168.2.0 0.0.0.127 area 0
 network 192.168.3.0 0.0.0.127 area 0
 network 192.168.4.0 0.0.0.127 area 0
 network 192.168.50.0 0.0.0.255 area 0
!
ip classless
access-list 2 permit 0.0.0.0 255.255.255.0
access-list 2 deny any
!
banner motd ^C^C
!
!
!
!
logging 10.20.20.6
line con 0
 exec-timeout 3 0
 password 7 0822455D0A16
 login
!
line aux 0
!
line vty 0 4
 access-class 2 in
 login local
 transport input ssh
line vty 5 15
 access-class 2 in
 login local
 transport input ssh
!
```

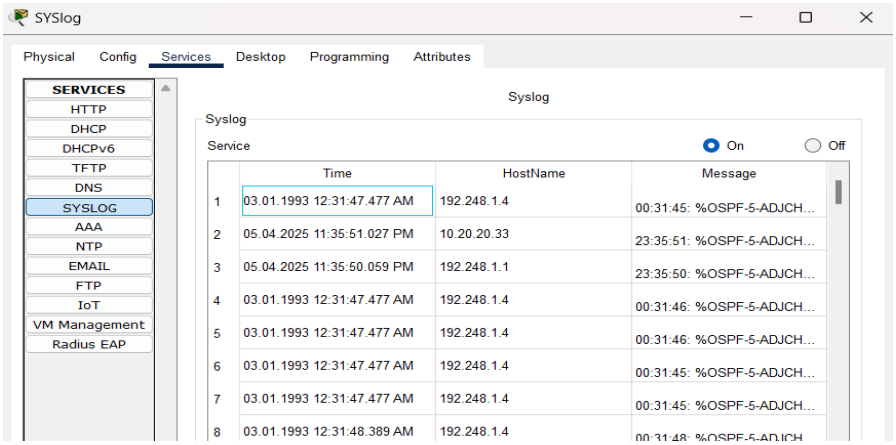
- ✓ The same configuration configured on HQ-DS2 MLS, OU-DSW1, OU-DSW2

HQ Switch configurations (Access layer)

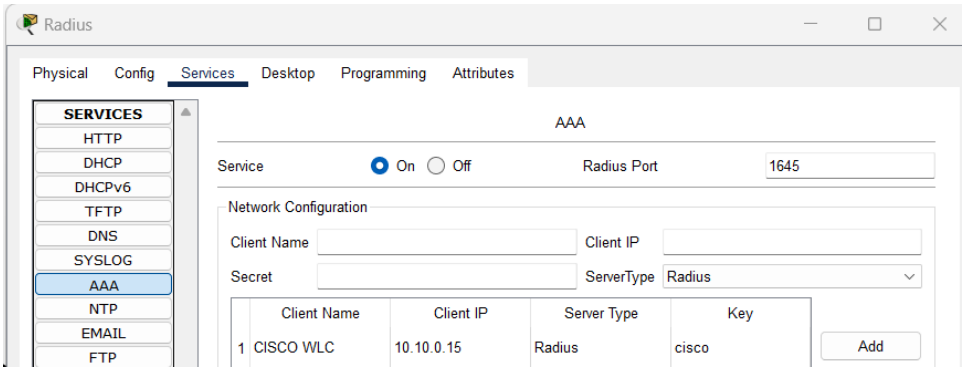


- ✓ The same configurations configured on HR Department, IT/Technical department, Finance department switches and outlet access layer switches

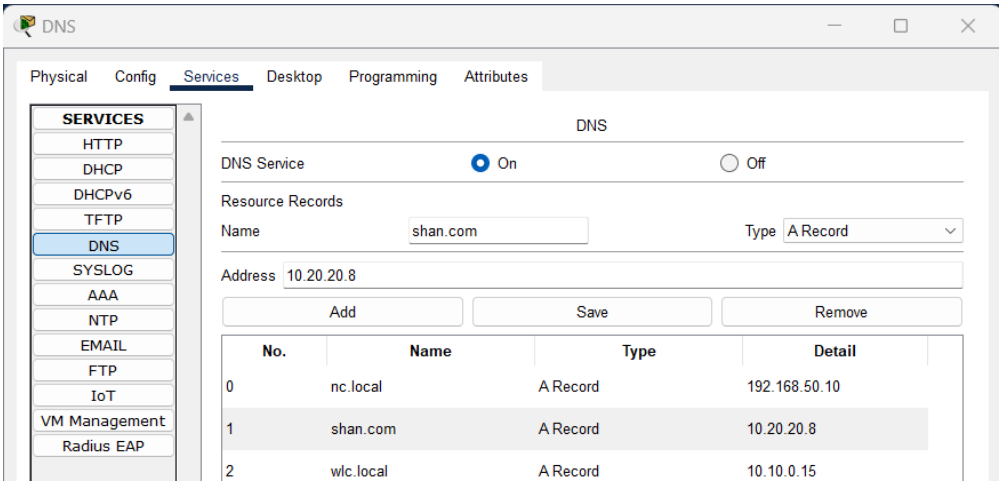
Syslog server



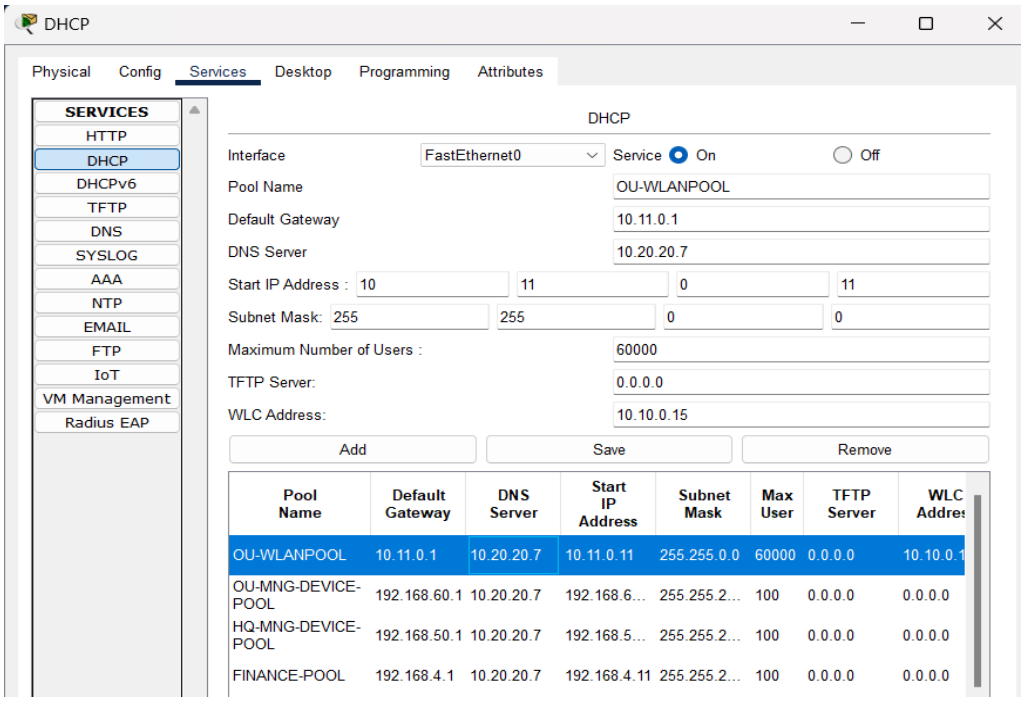
RADIUS Server



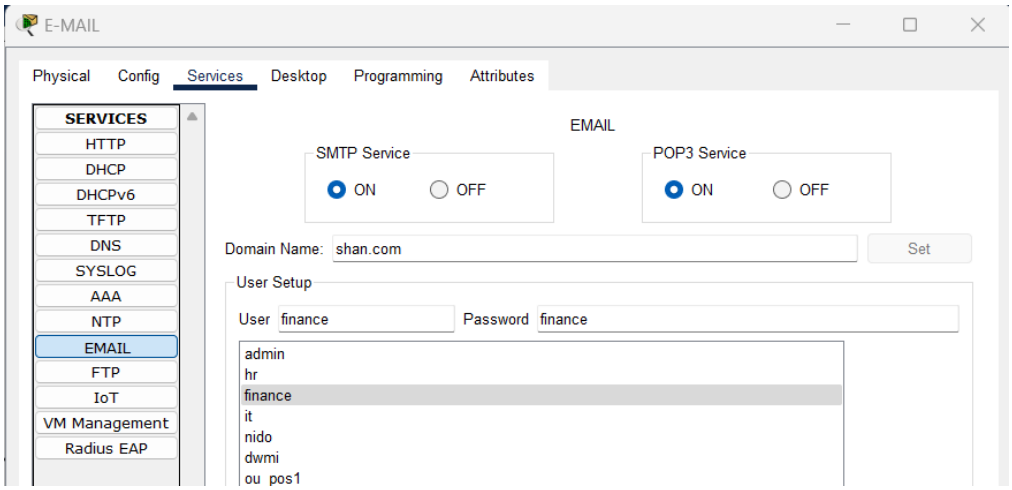
DNS Server



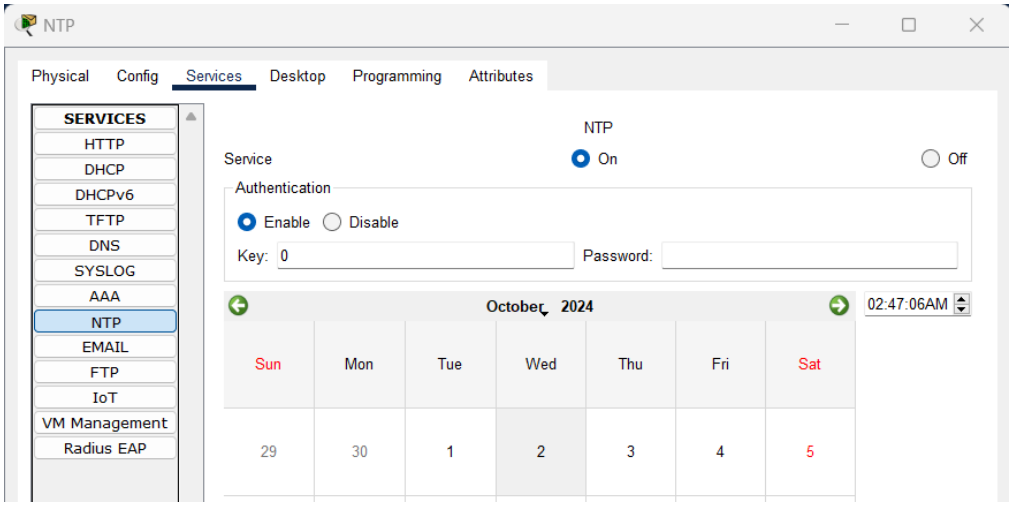
DHCP Server



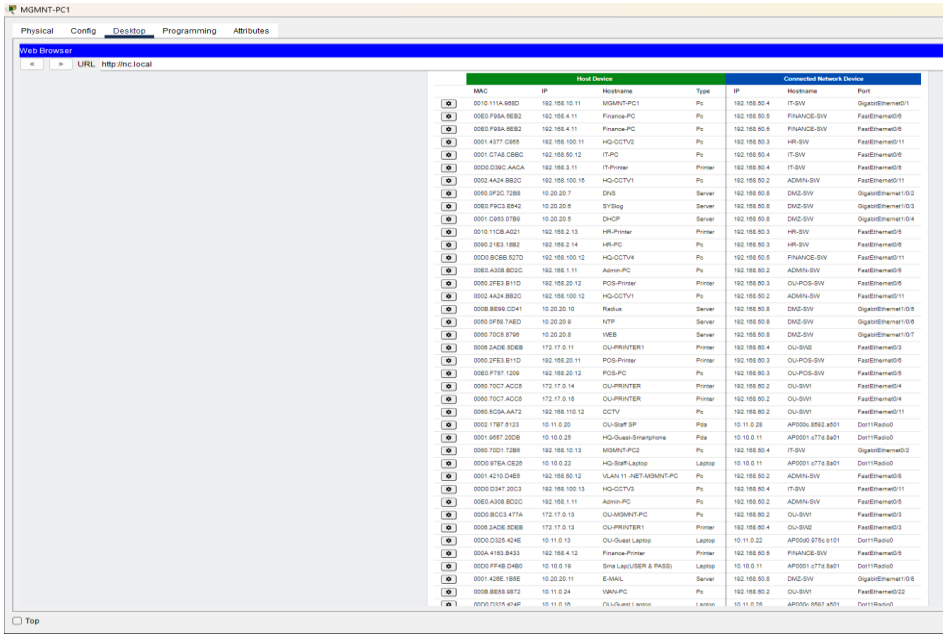
Email Server

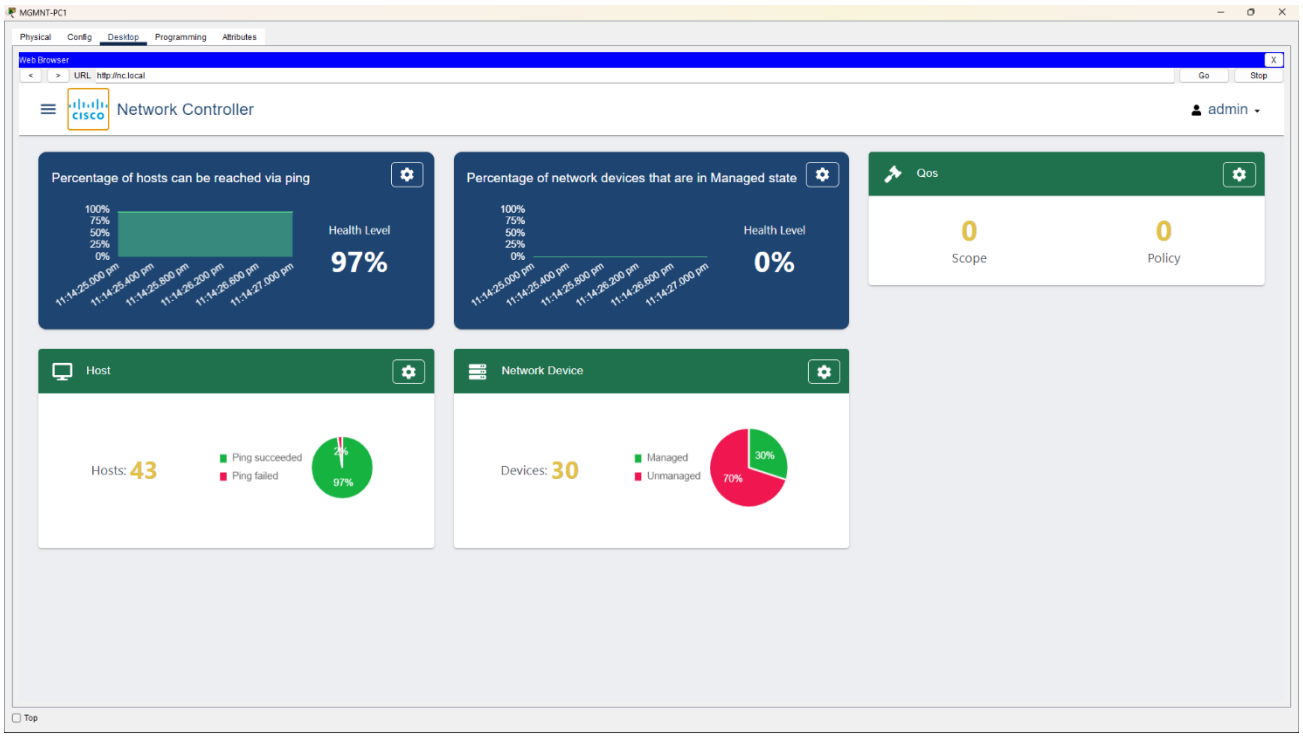


NTP Server



Network Controller





WLC

AP Group Name	AP Group Description	
HQ	HQ-USERS	Remove
OUTLET-GROUP	OUTLET-GROUP-USERS	Remove
default-group		

APs currently in the Group — Remove APs

AP Name	Ethernet MAC
0090.0CA3.850D	0090.0CA3.850D
HQ-ADMIN-AP	0001.C77D.8A01
HQ-IT-AP	00E0.F70D.2DA3
0009.7C37.DB98	0009.7C37.DB98

APs currently in the Group — Remove APs

AP Name	Ethernet MAC
OU-AP3	0001.9771.A801
OU-AP1	000C.8592.A501
OU-POS-AP	00D0.975C.B101
000B.BE39.87D0	000B.BE39.87D0
000D.BDBB.960B	000D.BDBB.960B
OU-AP2	0003.E40C.0B01
0090.21D0.61C7	0090.21D0.61C7

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies	
1	WLAN	Guest USERS	Guest WiFi	Enabled	[WPA2][Auth(PSK)]	Remove
2	WLAN	Staff Users	Staff WiFi	Enabled	[WPA2][Auth(PSK)]	Remove
3	WLAN	Outlet-Staffs	Ou_Staff_WiFi	Enabled	[WPA2][Auth(PSK)]	Remove
4	WLAN	Outlet-Customers	Customer_WiFi	Enabled	[WPA2][Auth(PSK)]	Remove
5	WLAN	Smart_Access	Smart_WiFi	Enabled	[WPA2][Auth(802.1X)]	Remove

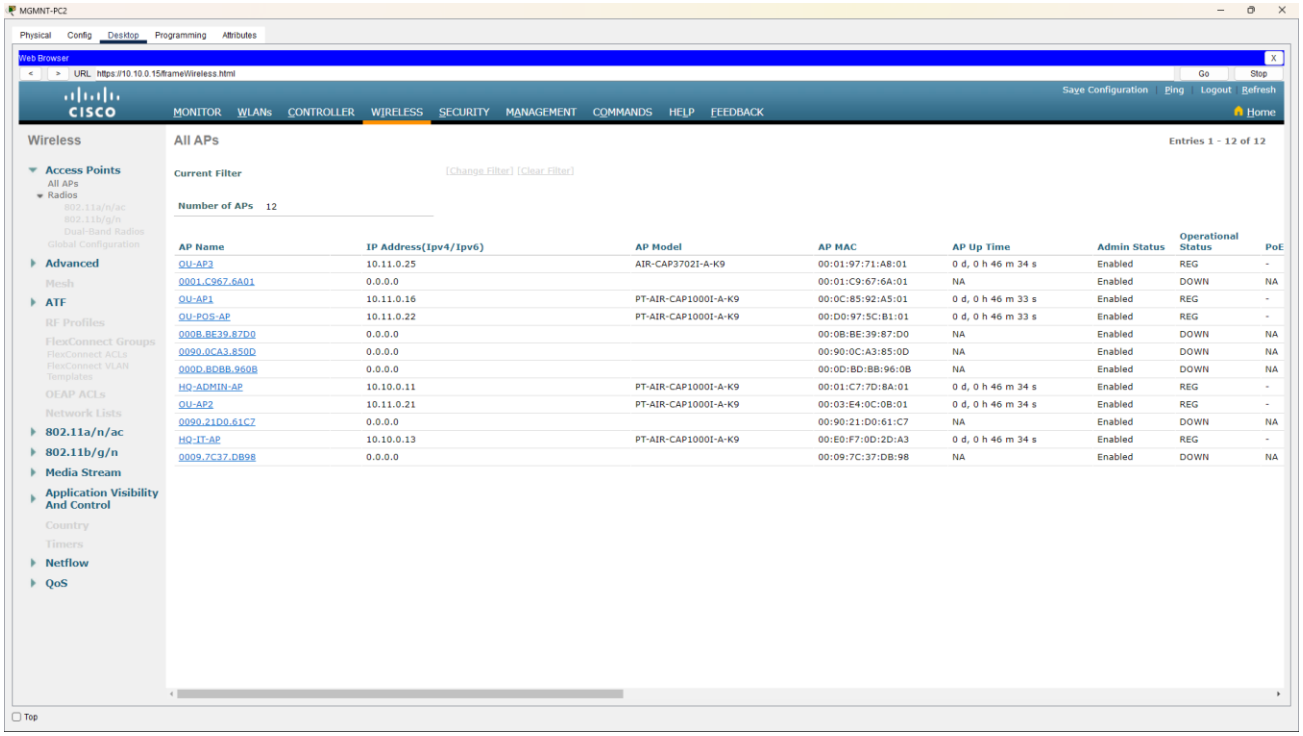
HQ-SSID-Group

WLAN ID	WLAN SSID[(2)(6)]	Interface/Interface Group(G)	SNMP NAC State	
1	Guest WiFi	management	Disabled	Remove
2	Staff WiFi	management	Disabled	Remove
5	Smart_WiFi	management	Disabled	Remove

OU-SSID-Group

Add New

WLAN ID	WLAN SSID[(2)(6)]	Interface/Interface Group(G)	SNMP NAC State	
3	Ou_Staff_WIFi	management	Disabled	Remove
4	Customer_WiFi	management	Disabled	Remove



Conclusion

The suggested enterprise network design effectively meets the current and future requirements of the supermarket chain by presenting a very secure, modular, and scalable solution. The Head Office (HQ) and Branch Outlet (OU) are linked through a site-to-site IPsec VPN to establish secure encrypted communication over public networks. The use of layered architecture (Edge, Distribution, Access) within the two sites improves manageability and boosts performance.

Centralized services such as DHCP, DNS, RADIUS, Email, and Syslog are located in the DMZ zone of the HQ, protected by stateful firewall policies and granular ACLs. The centralized model reduces administrative burden without any sacrifice in rigorous access control. VLAN-based segmentation between departments and functional areas separates the traffic, minimizes broadcast domains, and strengthens security posture. For example, critical systems such as VoIP and CCTV operate in their own isolated VLANs with QoS policies and voice VLAN tagging.

The distribution layers at Outlet and HQ are designed with redundancy, with HSRP and EtherChannel providing gateway failover and load-balancing. Routing between VLANs and networks is accomplished efficiently with OSPF, with dynamic route updates and fast convergence in the event of link failures.

Security is incorporated tightly within the design in a number of layers. These include:

- RADIUS authentication for wireless access.
- ACLs to control inter-VLAN and VPN traffic flow.
- Unused ports placed in a "blackhole" VLAN (199) and administratively shut down to prevent unauthorized access.

Network monitoring and logging enabled via a central Syslog server at HQ, with all major devices (firewalls, routers, switches) sending logs for auditing and fault detection.

Voice infrastructure is maintained through the use separate VoIP Gateway

Overall, this network design ensures **high availability, secure connectivity, simplified maintenance, and future scalability**, positioning the organization to meet future IT needs while ensuring business continuity and data integrity

Workload Matrix

#	Member Name	ID NO	Tasks Contributed
1	M. Nidosan	28177	Network Design, Configure, Testing and troubleshooting
2	Naveesha Thathsarani	28262	Documenting, Troubleshooting
3	Tharushi Dewmini	28428	VLAN planning and addressing, Testing
4	Shehan Kavinda	28928	Planning, and Network Design
5	K. Vinokrishnan	28778	Documentation and screenshots